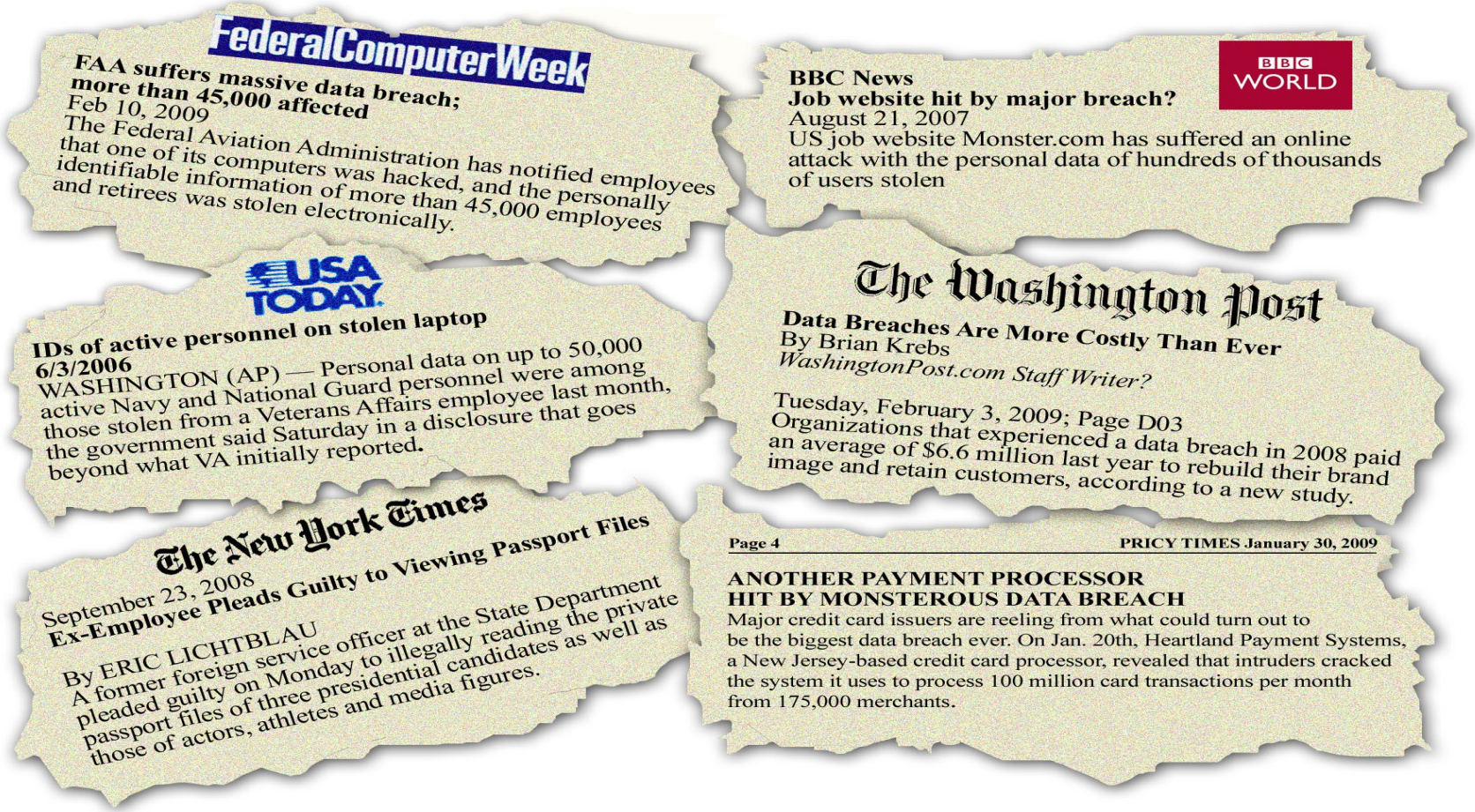
Presented by:
Gary Evans
Gary.Evans@osd.mil
703-699-0108
Office of the DoD CIO/NII
November 17, 2009

The Uphill Battle

Privacy in the News



Federal Computer Week

FAA suffers massive data breach; more than 45,000 affected
Feb 10, 2009
The Federal Aviation Administration has notified employees that one of its computers was hacked, and the personally identifiable information of more than 45,000 employees and retirees was stolen electronically.

BBC WORLD

BBC News
Job website hit by major breach?
August 21, 2007
US job website Monster.com has suffered an online attack with the personal data of hundreds of thousands of users stolen

USA TODAY

IDs of active personnel on stolen laptop
6/3/2006
WASHINGTON (AP) — Personal data on up to 50,000 active Navy and National Guard personnel were among those stolen from a Veterans Affairs employee last month, the government said Saturday in a disclosure that goes beyond what VA initially reported.

The Washington Post

Data Breaches Are More Costly Than Ever
By Brian Krebs
WashingtonPost.com Staff Writer?

Tuesday, February 3, 2009; Page D03
Organizations that experienced a data breach in 2008 paid an average of $6.6 million last year to rebuild their brand image and retain customers, according to a new study.

The New York Times

September 23, 2008
Ex-Employee Pleads Guilty to Viewing Passport Files

By ERIC LICHTBLAU
A former foreign service officer at the State Department pleaded guilty on Monday to illegally reading the private passport files of three presidential candidates as well as those of actors, athletes and media figures.

Page 4 PRICY TIMES January 30, 2009

ANOTHER PAYMENT PROCESSOR HIT BY MONSTEROUS DATA BREACH
Major credit card issuers are reeling from what could turn out to be the biggest data breach ever. On Jan. 20th, Heartland Payment Systems, a New Jersey-based credit card processor, revealed that intruders cracked the system it uses to process 100 million card transactions per month from 175,000 merchants.

http://www.wreg.com/wreg-stolenlaptop-story,0,4408113.story

Rising Threat of Identity Theft

- Thus far in 2009, the Identity Theft Resource Center estimates that nearly 13.5 MILLION data records have been compromised.

- According to an October 2009 Gallop poll, Identity Theft tops Americans' crime concerns.

- Asked how much they worry about a list of 12 different types of crime, Americans were most likely to say they worry frequently about:

    - Identity theft (31%)
    - Home burglarized (21%)
    - Car stolen or broken into (19%)

Sample FY 2009 Data Breaches in the Federal Government

- **11/08** - FEMA laptop with SSNs of dozens of Indiana flood victims stolen.
- **4/09** - National Archives cannot find external hard drive with 1 terabyte of data containing SSNs and home addresses of Clinton administration White House workers and visitors.
- **7/27/09** - Army Guard contractor lost a laptop containing SSNs and other data on participants in Army Guard bonus and incentive program, potentially affecting 131,000 current and former Guard members.
- **8/18/09** - Naval Hospital in Pensacola notified thousands of beneficiaries using pharmacy services when a laptop disappeared with a database of

Example PII Breaches

“Secure at the Conference?”

Example PII Breaches

"In Plain Site"

"The Convenience"

Example PII Breaches

“Laptops in Luggage”

“Eyes on Laptop”

Example PII Breaches

New Zealander discovered U.S. Military files on an MP3 he bought in a thrift shop.

On April 22, 2009 A thumb drive containing PII consisting of the names, ranks, social security numbers, dates of birth, and nationalities was lost (8000 records)

http://www.cnn.com/video/#/video/ech/2009/01/27/lavendera.nz.mp3.cnn

DoD Policy Memorandum "Encryption of Sensitive Unclassified Data at Rest On Mobile Computing Devices and Removable Storage Media," July 3, 2007

- DoD policy mandates encryption not only for PII records, but for all non-publicly released unclassified information that is contained on mobile computing devices and removable storage media.
- This policy was developed based upon previous DoD and OMB DAR encryption policies that specify a requirement for FIPS 140-2 cryptography.

Peer-to-Peer (P2P) File Sharing

- The popular software allows computer users to share music or other files and is easily available on line
- Uses of P2P:
  - Planned file sharing – its intended use
  - Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence
  - Distribution and sharing of illegal information
- Example applications: BearShare, eDonkey, KaZaA, LimeWire, and Morpheus
- Recent Breach: House Ethics Committee
- Bottom line: “P2P file-sharing continues to be a major security risk and privacy issue.”
  - - Testimony of Robert Boback, the Chief Executive Officer of Tiversa at a Congressional Hearing on July 29, 2009

Phishing

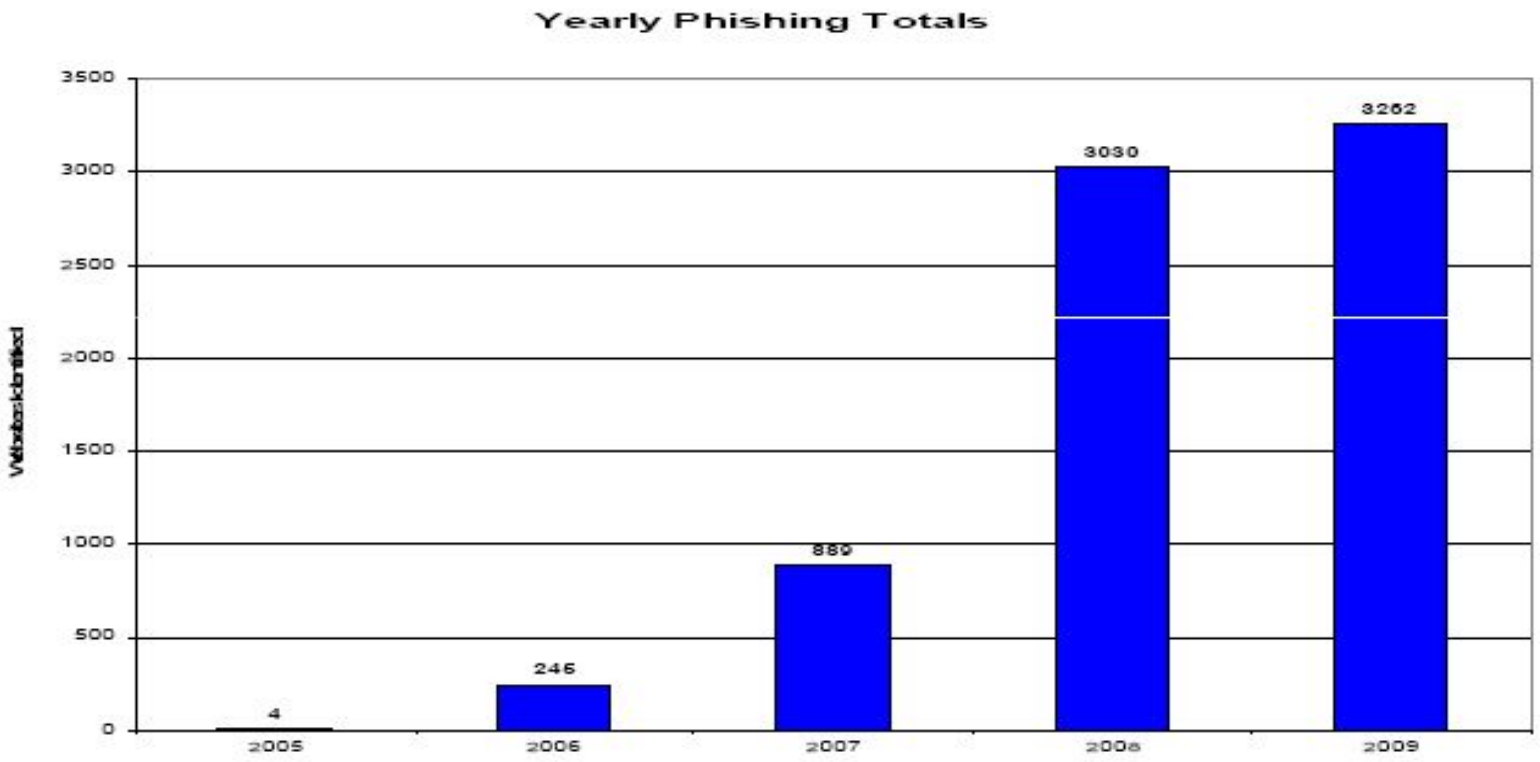
- **Phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

- Phishing is typically carried out by e-mail or instant messaging

- Never open emails from unknown sources or institutions soliciting personal information (SSNs)

IRS Phishing Statistics

Phishing Statistics by Year 2005-2009



phishing@irs.gov

* Through Oct 16, 2009

What Can Individuals do to Prevent ID Theft?

- Regularly check your credit record.
- Keep a purse or wallet in a safe place at work.
- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security Number. Don't carry a Social Security card in your wallet or write your Social Security Numbers on checks.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.

Social Media

http://www.facebook.com/video/video.php?v=141629337756&ref=share

PIAs Raise the Fundamental Question

What is a PIA?

- *"**Privacy Impact Assessment (PIA)--***is an analysis of how information is handled:
  - (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
  - (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and
  - (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." ***OMB 03-22 (9/26/2003), see EGOV 208(b)***

Essential Elements of the PIA

- What privacy information is collected
- Why the information is collected
- What the intended uses are for the information
- With whom the information is shared
- What opportunities individuals have to decline to provide PII
- How information is secured
- Whether a System of Records Notice (SORN) exists
- What privacy risks need to be addressed

Highlights of the DoDI 5400.16 PIA Guidance

- Formalizes E-Gov Act PIA requirement in DoD for greater visibility and clarity
- Better coordination with other processes
  - Privacy Act SORNs
  - Information Collection
  - Certification and Accreditation
  - Budget
- Establishes review cycle
- Structures privacy risk identification and assessment with new DoD PIA Form (DD 2930)

Highlights of the New PIA Template (DD Form 2930)

- More comprehensive tool
  - Detailed risk analysis questions
  - In-depth PII table for selection
  - Technical, administrative and physical control list provided
  - Interactive form with check boxes, radio buttons, and tables
  - Digital signatures for the PDF form
  - MS Word version also available

Privacy Risk Analysis

Summary

- Privacy and protection of personal information is important
- High visibility with OMB, Congress and GAO
- DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," located at:
- http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf

- DoD PIA FORM 2930 located at:
- http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage3438.html


Road to
Protection
You're the Drive

Backup Material

Privacy Related Security Awareness Training

- Personal Electronic Devices / Removable Storage Media.
  - http://iase.disa.mil/eta/pedrm/pedrm/index.htm
  - learn about the security risks associated with portable electronic devices and removable storage media
- Phishing
  - http://iase.disa.mil/eta/phishing/Phishing/launchPage.htm
- PII awareness
  - http://iase.disa.mil/eta/pii/pii_module/pii_module/index.html